

1 GABRIEL M. RAMSEY (STATE BAR NO. 209218)
gramsey@crowell.com
2 CHRISTOPHER CADENA (STATE BAR NO. 284834)
ccadena@crowell.com
3 CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
4 San Francisco, CA 94111
Telephone: 415.986.2800
5 Facsimile: 415.986.2827

6 Attorneys for Plaintiff MJ Freeway LLC
7
8
9

10 UNITED STATES DISTRICT COURT
11 NORTHERN DISTRICT OF CALIFORNIA
12 SAN FRANCISCO DIVISION
13

14 MJ FREEWAY LLC, a Colorado limited
liability company,

15
16 Plaintiff,

17 v.

18 JOHN DOE,

19 Defendant.
20
21
22
23
24
25
26
27
28

Case No. 3:18-cv-01828-JCS

**MJ FREEWAY LLC'S RENEWED
MOTION FOR LEAVE TO CONDUCT
THIRD PARTY DISCOVERY**

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND TO THEIR COUNSEL:

PLEASE TAKE NOTICE THAT Plaintiff MJ Freeway LLC (“MJ Freeway”) hereby moves this Court for an order granting leave to conduct third party discovery sufficient to identify, name and serve the John Doe Defendant in this action. Pursuant to the Motion to Shorten Time filed on March 23, 2018, MJ Freeway respectfully requests that the instant motion be heard on March 30, 2018 or as soon thereafter as the matter may be heard, so that MJ Freeway may more quickly learn of the John Doe Defendant’s identity and location and more quickly name them in this action.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiff MJ Freeway respectfully moves for leave to conduct the discovery necessary to identify the John Doe Defendant (“Defendant”) named in this action. MJ Freeway filed this lawsuit alleging violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030, *et seq.*), trade secret misappropriation under the Defend Trade Secret Act (18 U.S.C. § 1836, *et seq.*) and California’s Uniform Trade Secrets Act (Cal. Civ. Code § 3246, *et seq.*), unfair competition and other California state law claims, after it discovered that, at least as early as late 2016, and at several points thereafter, Defendant intentionally, and without authorization and exceeding authorization, accessed MJ Freeway’s computers and servers that store MJ Freeway’s confidential and proprietary material and disseminated that information.

Since learning of the unauthorized access of its computers and the disclosure of its confidential material, MJ Freeway has undertaken an extensive investigation to identify the individual(s) responsible for these unlawful actions. This investigation has resulted in identification of information used by Defendant to carry out the unauthorized intrusion and access, and to disseminate MJ Freeway’s confidential information, including electronic mail addresses, IP addresses, Internet domains, dedicated and cloud hosting facilities, social media accounts and similar technical infrastructure. MJ Freeway has searched public records and the Internet for information regarding this infrastructure that might lead to identification of the

Defendant. MJ Freeway has also requested information from competitors, former and current employees and third party consultants that might lead to identification of the Defendant. Notwithstanding these efforts, MJ Freeway has not been able to identify the Defendant. Having exhausted all reasonable efforts, MJ Freeway is, as yet, unable to determine the identity of the Defendant and the information that may definitively identify the Defendant appears to reside with third parties including Internet Service Providers, which maintain the records regarding the electronic mail addresses, IP addresses, internet domains, dedicated and cloud hosting facilities, social media accounts and similar technical infrastructure used by Defendant to carry out the unlawful actions at issue.

MJ Freeway now seeks leave to conduct limited discovery of third party entities, which maintain the records regarding the electronic mail addresses, IP addresses, internet domains, dedicated and cloud hosting facilities, social media accounts and similar technical infrastructure used by Defendant to carry out the unlawful actions at issue. This discovery is necessary to identify and locate the Defendant responsible for the unauthorized access of MJ Freeway's computers and dissemination of its confidential material.

II. FACTS

MJ Freeway is the industry-leading software, consulting, and data solution for cannabis businesses, serving clients in every regulated market in the United States, Canada, Europe, and Australia. Founded in 2010 and designed and built specifically for cannabis businesses, MJ Freeway's technology includes an innovative seed to sale supply chain Enterprise Resource Planning (ERP) Platform which leverages sophisticated business intelligence insights. MJ Freeway's pioneering Leaf Data Systems software solution enables governments to track cannabis, prevent diversion, and ensure patient, public, and product safety. MJ Freeway also offers a complete suite of consulting services for new and existing cannabis businesses. Complaint at ¶ 7.

A. Defendant, Without Authorization, Intruded Into MJ Freeway's Computers And Accessed Confidential Information

MJ Freeway stores its confidential and proprietary material on secured computers and

1 servers. MJ Freeway's computers and servers are accessible only by secure means and with
 2 authorization, via the Internet and local networks. *Id.*, ¶ 15. Beginning at least as early as late
 3 2016, and at several points thereafter, Defendant intentionally accessed MJ Freeway's computers
 4 and servers that store MJ Freeway's confidential and proprietary material without authorization or
 5 exceeding Defendant's authorization. *Id.*

6 MJ Freeway did not authorize Defendant to access its computers and servers to obtain this
 7 confidential and proprietary MJ Freeway information and trade secrets. *Id.*, ¶ 16. To the
 8 contrary, such information is only accessible to those employees and/or third party consultants
 9 that entered into an employment and/or consultant agreement that contained confidentiality, non-
 10 disclosure and non-use provisions. *Id.* Nor could Defendant use MJ Freeway's confidential,
 11 proprietary and trade secret material for its own benefit or to MJ Freeway's detriment, without
 12 MJ Freeway's consent. *Id.*

13 Defendant carried out the unauthorized intrusion and access to MJ Freeway's computers
 14 and servers, and created technical infrastructure to do so, using a variety of third party technical
 15 infrastructure, including electronic mail addresses, IP addresses, internet domains, dedicated and
 16 cloud hosting facilities, social media accounts and similar technical infrastructure. *Id.*, ¶ 15.
 17 Defendant carried out this unauthorized intrusion, through a variety of technical means, including
 18 transmission of a program, information, code and command, and the theft of credentials.
 19 *Id.*, ¶ 21.

20 **B. Defendant Disclosed MJ Freeway's Confidential And Proprietary**
 21 **Information To MJ Freeway's Competitors And To The Public**

22 MJ Freeway has expended tremendous resources to cultivate and develop valuable
 23 information and intellectual property. *Id.*, ¶ 8. MJ Freeway has spent significant time, effort and
 24 money since at least 2010 to develop valuable business trade secrets including, but not limited to
 25 computer code and program designs comprising MJ Freeway's software products, designs for its
 26 current and future products and technologies, research and development techniques and results,
 27 product and technology prototypes, product and technology specifications, schematics and similar
 28 descriptions, product components, customer and client information, business information and

1 other confidential intellectual property. *Id.* The development, refinement, compilation and
 2 management of such information have enabled MJ Freeway to succeed in a competitive industry.
 3 *Id.*

4 Defendant intentionally accessed MJ Freeway's computers and servers that store its
 5 confidential and proprietary material, copied confidential MJ Freeway material, including source
 6 code for its products and systems and confidential customer and client data, and transmitted said
 7 material to MJ Freeway's competitors and to the public. *Id.*, ¶ 14.

8 C. **MJ Freeway Has Exhausted All Reasonable Efforts To Identify And Locate**
 9 **Defendant**

10 Upon discovering that Defendant intentionally, and without authorization and exceeding
 11 authorization, accessed MJ Freeway's computers and servers that store MJ Freeway's
 12 confidential and proprietary material and disseminated that information, MJ Freeway undertook
 13 an extensive investigation to identify the individual(s) responsible for these unlawful actions,
 14 including their name and location. Declaration of Gabriel M. Ramsey ("Ramsey Decl."), ¶¶ 3-4.

15 MJ Freeway has undertaken an extensive technical investigation regarding the
 16 Defendant's intrusion into MJ Freeway's computers. This investigation has resulted in
 17 identification of information used by Defendant to carry out the unauthorized intrusion and
 18 access, and to disseminate MJ Freeway's confidential information, including electronic mail
 19 addresses, Internet Protocol ("IP") addresses, internet domains, dedicated and cloud hosting
 20 facilities, social media accounts and similar technical infrastructure. Ramsey Decl., ¶ 5

21 MJ Freeway has engaged in an extensive search of public records and the Internet for
 22 information regarding this infrastructure that might lead to identification of the Defendant. *Id.*, ¶¶
 23 6-14. MJ Freeway has also requested information from competitors, former and current
 24 employees and third party consultants that might lead to identification of the Defendant. *Id.*, ¶ 15.
 25 To date, no information sufficient to definitively identify and name the Defendant has been
 26 obtained from public resources associated with the technical infrastructure used by Defendant, or
 27 from other public sources. *Id.*, ¶¶ 6-15.
 28

D. Civil Discovery Is Likely To Enable MJ Freeway To Identify The Defendant Responsible For Accessing Its Computers And Disclosing Its Confidential Intellectual Property And Trade Secrets

Through its investigation, MJ Freeway has identified the following technical infrastructure associated with the Defendant and which Defendant used to carry out the acts alleged in the Complaint. Discovery to, at least, the following sources of information is reasonably likely to enable MJ Freeway to identify Defendant:

- a) Defendant used the email account **jvauvl@gmail.com** to create an administrative account to impersonate an MJ Freeway employee and obtain unauthorized access to MJ Freeway's computers. Discovery to the email address provider is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including IP addresses used at a particular date and time by Defendant to register and access the account. Ramsey Decl., ¶ 6.a., Ex. 1.
- b) Defendant used the following accounts on the social media site reddit.com to distribute MJ Freeway's confidential and trade secret source code: **techdudes420**, **deerd0e1962**, **superyonnie**. Discovery to the provider of these accounts is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including IP addresses used at a particular date and time by Defendant to register and access the accounts. *Id.* at ¶ 6.b., Ex. 2.
- c) Defendant installed malicious software on a server of MJ Freeway and used the malicious software to send information from that server to the domain mjfreewayzone.com. Defendant used the email account **thecontroller82@juno.com** to register the foregoing domain. Discovery to the email address provider is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including IP addresses used at a particular date and time by Defendant to register and access the account. *Id.* at ¶ 6.c., Ex. 3.

- d) Defendant logged into the email account **mjdatasales@juno.com** from a server used by Defendant to carry out the intrusion against MJ Freeway. Discovery to the email address provider is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including IP addresses used at a particular date and time by Defendant to register and access the account. *Id.* at ¶ 6.d., Ex. 3.
- e) The Defendant accessed MJ Freeway's confidential and trade secret source code on **bitbucket.org**, a code repository site, and created an account at that site using the email account: **thecontroller82@juno.com**. Discovery to the code repository provider regarding the account registered with this email address is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including IP addresses used at a particular date and time by Defendant to register and access the account. *Id.*, ¶ 6.e., Ex. 4.
- f) Defendant used the following accounts on the social media site twitter.com to distribute MJ Freeway's confidential and trade secret source code: **noonerunthispl** and **runthisplace**. Discovery to the provider of these accounts is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including IP addresses used at a particular date and time by Defendant to register and access the accounts. *Id.*, ¶ 6.f., Ex. 5.
- g) Defendant used the Amazon Web Services cloud computing account: **arn:aws:iam::311152497758:user/theodo**, to make unauthorized access to MJ Freeway's computers and the confidential data on those computers. Discovery to the provider of this account is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including IP addresses used at a particular date and time by Defendant to register and access the accounts. *Id.*, ¶ 6.g., Ex. 6.

- h) Defendant created the following account on github.com, a code repository site, to distribute MJ Freeway's confidential and trade secret source code: **mjfreeway**. Discovery to the provider of this account is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including IP addresses used at a particular date and time by Defendant to register and access the account. *Id.*, ¶ 6.h., Ex. 7.
- i) Defendant created the following account on gitlab.com, a code repository site, to distribute MJ Freeway's confidential and trade secret source code: **mjfreeway**. Discovery to the provider of this account is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including IP addresses used at a particular date and time by Defendant to register and access the account. *Id.*, ¶ 6.i., Ex. 8.
- j) Defendant registered the Internet domain **mjfzone.net** and associated account to distribute MJ Freeway's confidential and trade secret source code. Discovery to the domain registrar through which this account was registered is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including payment information and IP addresses used at a particular date and time by Defendant to register and access the account. *Id.*, ¶ 6.j., Ex. 9.
- k) Defendant registered the Internet domain **marihuanadata.com** and associated account to distribute MJ Freeway's confidential and trade secret source code. Discovery to the domain registrar through which this account was registered is likely to reveal information about the Defendant's identity, such as account registration information, and/or information that, with further discovery, will lead to Defendant's identity, including payment information and IP addresses used at a particular date and time by Defendant to register and access the account. *Id.*, ¶ 6.k., Ex. 10.
- l) Defendant used the email account **weselludata@mail2world.com** to distribute MJ Freeway's confidential and trade secret source code. Discovery to the email address

1 provider is likely to reveal information about the Defendant's identity, such as account
2 registration information, and/or information that, with further discovery, will lead to
3 Defendant's identity, including IP addresses used at a particular date and time by
4 Defendant to register and access the account. *Id.*, ¶ 6.1., Ex. 11.

5 The third party technical infrastructure providers who maintain these accounts and
6 technical facilities are reasonably likely to be in possession of information that would identify
7 Defendant. Internet electronic mail providers, Internet Service Providers that allocate IP
8 addresses, domain registrars and resellers through which Internet domains are sold, dedicated
9 hosting companies and cloud computing companies that provide servers that host code or
10 domains, social media account providers and other similar infrastructure providers, including the
11 foregoing, require that users of their services provide certain information when they sign up. For
12 example, users may be required to provide information such as a name, address, age, postal code
13 and an alternative email address, and payment instrument information, so that the infrastructure
14 provider may contact the potential user about their accounts and infrastructure. Although a user
15 might falsify some such information, they may also provide information that is actually in use,
16 such as an alternative email address, and such infrastructure providers can use such points of
17 contact to send the user important account-related information. *Id.*, ¶ 7.

18 Infrastructure providers also often record IP addresses used to register or to access such
19 accounts. Once these IP addresses are identified, they may be used to identify accountholders.
20 Specifically, to access the Internet, computers need an IP address, which enables computers to
21 identify and communicate with other computers over the Internet. Internet Service Providers
22 lease IP addresses to individuals and businesses, typically in conjunction with Internet access
23 service. The header and transmission data of email should also contain the IP address for the
24 computer at a particular date and time as well as the IP address for the Internet Service Provider
25 that the email was routed through. Internet Service Providers frequently have records identifying
26 the individuals who purchased, signed up for and used their services, or records that can lead to
27 the discovery of that information. For example, the Internet Service Providers generally will
28 maintain logs of which accountholder used a particular IP address at a given time. *Id.*, ¶ 8.

Thus, once IP addresses used by Defendant in this case are discovered, by subpoenas to the particular identified infrastructure providers set forth above, it is and will be possible to obtain further discovery from the third party companies controlling such IP addresses, to identify Defendants. This, in turn may also lead to further technical infrastructure (IP addresses, computer-specific addresses or other indicia of access or identity) as well as other payment or account information, all of which are reasonably likely to identify the Defendant. In particular, infrastructure providers may have other information to identify an accountholder, as they may have insisted on valid billing information, such as valid credit card or bank account data, and they will often retain records that demonstrate who paid for their services. Therefore, electronic payment processors, banks and other financial institutions are likely to be in possession of information sufficient to identify accountholders using a particular IP address or other technical infrastructure. Similarly, electronic mail providers, including the providers of the email infrastructure set forth above, often possess archived email “header” information, which includes, beyond IP addresses, other transmission data and routing information concerning from where email messages originated and to where they may be sent. This information enables the same form of investigation and identification of Defendant’s identity. *Id.*, ¶ 9.

Informal contact with third-party infrastructure providers or financial institutions whose services were used by Defendant to carry out the activities detailed in the complaint is unlikely to yield sufficient identifying information for Defendant. Such operators, including specifically the operators of the infrastructure above, typically refuse to divulge information about users or accounts without a subpoena or other legal authorization. *Id.*, ¶ 14. If granted civil discovery to investigate these sources of information, MJ Freeway will likely be able to obtain valid information leading to the identity of the Defendant.

III. ARGUMENT

MJ Freeway seeks leave of the Court to conduct discovery to determine the identity of the Doe Defendant so that they can be named in the complaint and the summons can be served upon them. The Ninth Circuit permits discovery to determine the identity of unknown defendants: “Where the identity of alleged defendants will not be known prior the filing of a complaint[,] ...

1 the plaintiff should be given an opportunity through discovery to identify the unknown
 2 defendants, unless it is clear that discovery would not uncover the identities, or that the complaint
 3 would be dismissed on other grounds.” *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980);
 4 *see also Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999) (relying on *Gillespie* in
 5 reversing district court’s dismissal of Doe complaint). In *Columbia Ins. Co. v. Seescandy.com*,
 6 185 F.R.D. 573 (N.D. Cal. 1999), the court suggested a four-part framework for a party’s motion
 7 for leave to conduct discovery against Doe defendants. *Id.* at 578.

8 Here, MJ Freeway’s third party discovery request is justified under *Gillespie* and the
 9 *Seescandy.com* framework. MJ Freeway therefore respectfully asks the Court to grant MJ
 10 Freeway leave to conduct limited discovery to locate and identify the Doe Defendant.

11 **A. Defendants Are Real Persons Or Entities**

12 Under *Seescandy.com*, MJ Freeway must first identify the missing party with sufficient
 13 specificity such that the Court can determine that the defendant is a real person or entity who
 14 could be sued in federal court. *Seescandy.com*, 185 F.R.D. at 578 (*citing Wells Fargo & Co. v.*
 15 *Wells Fargo Express Co.*, 556 F.2d 406, 430 n. 24 (9th Cir. 1977)). Here, the Doe Defendant is
 16 an individual or entity that has accessed MJ Freeway’s computers without authorization and has
 17 obtained confidential intellectual property and trade secrets. In doing so, Defendant
 18 misappropriated MJ Freeway’s trade secrets by, among other things, disclosing that information
 19 to MJ Freeway’s competitors and to the public. Defendant’s unauthorized access to and
 20 disclosure of MJ Freeway’s confidential intellectual property and trade secrets has caused MJ
 21 Freeway to incur damages and losses, including impairment to its computer systems, costs
 22 associated with investigating Defendant’s unauthorized computer access, as well as the loss to its
 23 business stemming from the diminished value of its trade secrets and associated goodwill.

24 Given the sophisticated and volitional nature of the illegal acts at issue, there can be no
 25 question that the Defendant is a real person or entity. The Defendant carried out the unlawful acts
 26 at issue using the specific technical infrastructure set forth above. In doing so, Defendant had to
 27 register and maintain this particular infrastructure, including providing identifying information to
 28 the infrastructure providers. Thus, Defendant is a discernible missing party, who is identified

with specificity by reference to the particular infrastructure that Defendant set up and used to carry out the illegal acts in the complaint. Once identified, through discovery to the providers of this infrastructure or further identified infrastructure, the Defendant will be subject to this lawsuit in federal court.

B. MJ Freeway Has Taken Substantial Steps To Locate The Defendant

The second *Seescandy.com* requirement is that MJ Freeway “identify all previous steps taken to locate the elusive defendant.” *Seescandy.com*, 185 F.R.D. at 579 (*citing Plant v. Does*, 19 F. Supp. 2d 1316 (S.D. Fla. 1998)). MJ Freeway’s efforts to date are substantial. *See Ramsey Decl.*, ¶¶ 5-15. After learning of the authorized access to its computers and servers, and disclosure of its confidential material and trade secrets, MJ Freeway undertook an investigation to identify and locate Defendant. *Id.*, ¶¶ 3-4. MJ Freeway carried out extensive technical investigation of the intrusion, which led to the identification of technical infrastructure, set forth above, used by Defendant to carry out the attack. *Id.*, ¶¶ 5-6. Thereafter, MJ Freeway searched public records and the Internet for evidence associated with the technical infrastructure, in an attempt to identify the Defendant. *Id.*, ¶¶ 6-14. MJ Freeway also has engaged with current and former employees, and with competitors, in an attempt to identify the Defendant. *Id.*, ¶ 15. To date, these efforts have not yielded any information sufficient to identify and name the Defendant. *Id.*, ¶ 15.

The technical information identified to date, that was used by the Defendant to carry out attacks, only has value when correlated with the accountholder information or other technical information in the possession of third party infrastructure providers. MJ Freeway seeks leave of the Court to issue discovery requests to such third parties because informal contact with those parties is unlikely to yield sufficient identifying information for the Defendant. *Id.*, ¶¶ 6-14. These entities typically refuse to divulge customer information without a subpoena or other legal authorization. *See id.* Accordingly, MJ Freeway respectfully requests that the Court grant MJ Freeway leave to serve discovery to such third parties. The requested discovery is necessary to identify the Doe Defendant carrying out the illegal conduct at issue in this case.

1 **C. MJ Freeway’s Action Can Withstand A Motion To Dismiss**

2 The third *Seescandy.com* factor requires MJ Freeway to establish, to the Court’s
 3 satisfaction, that its action against the Defendant can withstand a motion to dismiss.
 4 *Seescandy.com*, 185 F.R.D. at 579 (citing *Gillespie*, 629 F.2d at 642). MJ Freeway asserts claims
 5 stemming from Defendant’s violation of the Computer Fraud and Abuse Act (“CFAA”), trade
 6 secret misappropriation under the federal Defend Trade Secrets Act and California’s Uniform
 7 Trade Secrets Act, as well as unfair competition under state law and violation of California’s anti-
 8 hacking statute. Complaint, ¶ 1. MJ Freeway meets this requirement because, as pled in the
 9 Complaint in detail, there is technical evidence of Defendant’s unauthorized intrusion into MJ
 10 Freeway’s protected computers and servers, used in interstate and foreign commerce, as well as
 11 delivery of damaging code, and resultant unauthorized access to and disclosure of MJ Freeway’s
 12 confidential information and trade secrets.

13 **1. Violation Of The Computer Fraud And Abuse Act**

14 To state a claim for relief for a violation of the Computer Fraud and Abuse Act, MJ
 15 Freeway must plead facts that show Defendants (1) accessed a “protected computer,” (2) without
 16 authorization or in excess of authorization, (3) intentionally, and (4) as result of the conduct
 17 caused damages. *Multiven, Inc. v. Cisco Systems, Inc.*, 2010 WL 288962, *3 (N.D. Cal. July 20,
 18 2010).

19 MJ Freeway alleges in its Complaint that, without authorization, Defendant accessed MJ
 20 Freeway’s computers and servers (connected to the Internet) that contained confidential
 21 intellectual property and trade secrets and disclosed that material to MJ Freeway’s competitors
 22 and to the public, including by posting the material in internet forums and transmitting it by
 23 electronic means. Complaint, ¶¶ 14-25. MJ Freeway also alleges that Defendant’s access was
 24 unauthorized as they accessed MJ Freeway’s computers with the intent to disclose MJ Freeway’s
 25 confidential and proprietary material to third parties. *Id.* MJ Freeway further alleges that it has
 26 suffered damages and costs in excess of \$5,000, including costs associated with investigating the
 27 unauthorized access, mitigating the intrusion, and impairment to its computers and systems. *Id.*
 28 Accordingly, MJ Freeway has alleged sufficient facts to survive a motion to dismiss. *See*

1 *Multiven*, 2010 WL 288962 at *3-*5.

2 **2. Violation Of California Penal Code Section 502(c)**

3 Like the CFAA. Section 502(c) prohibits the unauthorized access of a computer. *Id.* at *6.
 4 MJ Freeway's claim under Section 502(c) is based on the same operative facts alleged in its claim
 5 for violation of the CFAA. Complaint, ¶¶ 14-25, 54-57. As MJ Freeway has alleged facts to state
 6 a claim for violation of the CFAA, it has also alleged facts to state a claim under Section 502(c).
 7 *Multiven*, 2010 WL 288962 at *6.

8 **3. Trade Secret Misappropriation**

9 To sustain a cause of action for trade secret misappropriation under the Defend Trade
 10 Secrets Act ("DTSA"), and California's Uniform Trade Secret Act ("CUTSA"), a plaintiff must
 11 allege facts that show: (1) the existence of a trade secret, (2) that the defendant either (a) acquired
 12 the plaintiff's trade secret through improper means or disclosed it third parties without the
 13 plaintiff's permission or (b) disclosure or use of the plaintiff's trade secret, acquired through
 14 improper means, without the plaintiff's consent. *See* 18 U.S.C. § 1836 *et seq.*; Cal. Civ. Code §
 15 3426.1; *Veronica Foods Co. v. Ecklin*, 2017 U.S. Dist. LEXIS 101325, at *41-42 (N.D. Cal. June
 16 29, 2017) (noting that "the DTSA and CUTSA's definitions of 'trade secret,' 'misappropriation,'
 17 and 'improper use' are substantially identical.")

18 MJ Freeway alleges in its Complaint that it has developed trade secrets, including its
 19 confidential intellectual property regarding its software, code, products, systems, user and
 20 customer information and business information. MJ Freeway further alleges that it employs
 21 passwords and other technological measures to limit access to its confidential material and that it
 22 employs confidentiality, non-disclosure and non-use agreements to protect such trade secrets. MJ
 23 Freeway alleges that, either by virtue of their unauthorized access and/or, directly or indirectly,
 24 their contractual or other obligations to MJ Freeway, that Defendant improperly obtained the
 25 trade secrets through technical means and/or through breach of a duty to maintain the secrecy of
 26 the trade secrets. MJ Freeway alleges that Defendant copied MJ Freeway's trade secrets with the
 27 intent to disclose them to MJ Freeway's competitors and to the public; and disclosed MJ
 28 Freeway's trade secrets to its competitors and to the public. Complaint, ¶¶ 8-18, 26-44. MJ

Freeway also alleges damages as a result of Defendant's misappropriation of MJ Freeway's trade secrets. *Id.* Thus, MJ Freeway states a claim for trade secret misappropriation.

4. Unfair Competition

California's unfair competition law prohibits "any unlawful, unfair, or fraudulent business act or practice." *Multiven*, 2010 WL 288962 at *7. An unfair competition plaintiff must show that it has lost money or property as a result of unfair competition. *Id.* In its Complaint, MJ Freeway alleges that Defendant engaged in unlawful conduct, i.e., the unauthorized access of its computers and servers in violation of the Computer Fraud and Abuse Act and Section 502(c) of California's Penal Code. Complaint, ¶¶ 14-25, 54-57. MJ Freeway also alleges that Defendant's unlawful conduct was intentional and constituted an unfair competition and trade secret misappropriation, as Defendant disclosed confidential MJ Freeway material to its competitors with the intent to injure MJ Freeway competitively. *Id.*, ¶¶ 26-53. MJ Freeway further alleges that it suffered damages, including the costs associated with investigating Defendant's unauthorized access and disclosure, conducting a damages assessment, taking mitigation measures and implementing additional security and safety measures to prevent further unauthorized access or disclosure. *Id.*, ¶¶ 17, 24. In sum, based on the allegations in its Complaint regarding the unlawful intrusion into and access to confidential MJ Freeway intellectual property and trade secrets stored on its computers, and disclosure of that intellectual property and trade secrets to MJ Freeway's competitors and to the public, MJ Freeway's lawsuit can survive a motion to dismiss.

D. MJ Freeway's Proposed Discovery Will Likely Lead To Identifying Information About Defendants

The final *Seescandy.com* factor requires MJ Freeway to support its request for discovery with reasons justifying the specific discovery requested, as well as the sources of discovery upon which process might be served. *Seescandy.com*, 185 F.R.D. at 579 (citing *Gillespie*, 629 F.2d at 642). In doing so, MJ Freeway should show that "there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible." *Id.* Here, as described above, MJ Freeway proposes a course of discovery that

will likely result in the identification of the Doe Defendant. MJ Freeway has identified above the specific technical infrastructure set up and used by Defendant to carry out the illegal acts in the Complaint. MJ Freeway proposes to serve discovery on the third party entities which provision and operate the above-described technical infrastructure. Proposed subpoenas, set forth at Exhibits 1-11 of the Ramsey Decl., seek from these third parties all information relating to the Defendant who registered, paid for and used the infrastructure that was used to carry out the attack against MJ Freeway. Recognizing that these entities may only be the first step in an investigation that ultimately leads to the identification of the Defendant, MJ Freeway requests authority to issue follow-up discovery on the leads provided by the initially subpoenaed parties controlling the infrastructure used by the Defendant. For example, subpoenas to the infrastructure providers who maintain the infrastructure listed above is likely to yield further IP addresses, email addresses and payment information, which would be the subject of follow up discovery. This approach to unknown defendants, using civil discovery to pursue account information and associated technical information, including follow up discovery on additional discovery leads that are uncovered, has been utilized in numerous prior matters to identify unknown defendants engaged in hacking activity. Ramsey Decl., ¶ 7. Such discovery and this approach has been successfully applied with respect to a number of the specific third parties that maintain the discovery at issue. *Id.* Accordingly, based on the known specific infrastructure at issue in this case, the fact that it is specifically identified with Defendant, the fact that the infrastructure providers are known to possess relevant information, and the fact that this civil discovery approach has led to successful identification of similarly situated defendants in the past, granting MJ Freeway leave to conduct discovery to the providers of the foregoing infrastructure (Ramsey Decl., Exs. 1-11) is reasonably likely to identify Defendant in this matter such that service of process would be possible.

Assuming timely responses to its proposed subpoenas at Ramsey Decl., Exs.1-11, and further assuming at least one round of additional follow-on discovery and timely response to any such subpoenas and any Letters of Request pursuant to the Hague Convention, if necessary, MJ Freeway expects to complete the Doe discovery phase in 180 days. These efforts are reasonably

likely to lead to identification and location of the Doe Defendant.

IV. CONCLUSION

For the foregoing reasons, MJ Freeway respectfully requests that the Court grant MJ Freeway's Renewed Motion for Leave to Conduct Third-Party Discovery.

Dated: March 28, 2018

CROWELL & MORING LLP

/s/ Gabriel M. Ramsey

GABRIEL M. RAMSEY
CHRISTOPHER CADENA
Attorneys for Plaintiff
MJ Freeway LLC